

**REMARKS OF WILLIAM J. FOX, DIRECTOR
THE FINANCIAL CRIMES ENFORCEMENT NETWORK
UNITED STATES DEPARTMENT OF THE TREASURY**

**THE 22ND CAMBRIDGE INTERNATIONAL SYMPOSIUM
ON ECONOMIC CRIME
THE FINANCIAL WAR ON TERROR AND ORGANIZED CRIME**

MONDAY, SEPTEMBER 6, 2004

Let me say first how much I appreciate the opportunity to be part of the 22nd annual Cambridge International Symposium on Economic Crime. I am honored to share keynote responsibilities this morning with such a distinguished panel of luminaries. It is also great to have the opportunity to interact with the many other participants of this Symposium. It is often the case that the conversations that occur on the side at events like this are as important as the formal presentations. True to the tradition of this great University, this Symposium is known the world over for its depth of intellectual pursuit. This Symposium has stood one of the most important tests of relevance in a global environment where financial crime has become a “hot topic”; an environment where one could attend a money laundering conference on any day of the week somewhere in the world. That test is the test of time. I salute Professor Barry Rider, Saul Froomkin and Jesus College for the foresight in establishing a symposium that has consistently brought together the very best people to discuss the right issues at the right time.

I last walked the hallowed grounds of Jesus College as a staffer for David Aufhauser, then General Counsel of the Treasury. On September 10, 2001, David provided a Monday keynote address and after thoroughly enjoying our time here, David and I hastily made our way back to Heathrow for a flight out the next morning . . . September 11, 2001. While waiting for our gate to be called, I glanced up at the screen and saw flights to the States methodically being cancelled – one by one. Thinking there was a hurricane on the East Coast, we found a United Airlines ticket agent who looked up at us – in tears – and told us that the United States was under attack. She told us the twin towers in New York were down, and the Pentagon in Washington had been blown up. You can only imagine the shock. After reaching our families, and confirming loved ones were still alive and well, we hopped a cab for Central London to find a hotel room somewhere close to the U.S. Embassy. On the way in, we tried to imagine how the world and our lives would change. We had no clue.

As I am sure many of you know, the Commission chartered by the United States Congress to review the events that led to the September 11th terrorist attacks has recently finished its work of reviewing the systemic breakdowns in intelligence gathering and

information sharing that prevented detection of both the plan to attack the World Trade Center, as well as the on-the-ground activities of the terrorists in the United States in the months leading up to the event. Much of the Commission's report necessarily deals with processes unique to the American political and governmental structure. Today, I would like to focus on the financial aspects of that attack – a topic to which the Commission gave less attention than almost any other. What have we learned from the financial aspects of the attack? Specifically, what are we to do about funds that fueled a monumental act of terrorism – especially when you consider that these funds were moved and used by terrorists under our very noses without detection?

The 9/11 Commission's principal recommendation relating to targeting terrorist money is clear: "[v]igorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts." I, for one, enthusiastically and wholeheartedly agree with this recommendation, and I agree with the Commission that the principal value of focusing on terrorist financing is to use financial flows to identify, locate, capture, and disrupt terrorists and their networks. That is not to diminish the efforts we and others have taken to choke off the funding of terrorist organizations, or other efforts to generally increase financial transparency to better protect the world's financial system. However, the Commission's conclusion is based upon the simple fact that many of us have known or suspected for some time – the fact that financial transactions remain an Achilles heel for terrorists and their organizations. Money – albeit often in very modest amounts – is needed to carry out terrorist operations, and money trails leave footprints. These trails connect dots – establishing previously unknown connections – so that organizations and networks can be defined and attacked. And most of the time, the money trails do not lie. Information in financial transactions is, for obvious reasons, generally reliable and, therefore, valuable to law enforcement and intelligence operatives. As we have developed and shared financial information throughout our government and between governments, we have learned that these trails are critical ways our law enforcement and security services can identify, locate, and arrest or capture terrorists, their networks and their supporters.

But in order to track money, you need information. A great deal of this information is obtained overtly, through laws promoting financial transparency, such as the Bank Secrecy Act of 1970 in the United States. For over 30 years, the United States Treasury Department has administered this Act to address very different problems other than tracking terrorist financing. The Act is implemented to seek information to identify and address money laundering – the efforts to take large sums of cash derived from illicit activity and “clean” it through a set of financial transactions so that dirty money appears legitimate. Tracking terrorist financing usually involves the movement of money – often clean money and often money in relatively modest amounts – to support an evil criminal purpose. Another way to put it – with money laundering, investigators look through a telescope trying to watch the movement of big amounts of dirty cash. With terrorist financing, investigators need a microscope, trying to watch the movement of often very small amounts of cash to support evil people attempting to achieve an evil purpose.

Think of it – a little over \$400,000 financed one of the most devastating terrorist attacks ever. This amount financed everything from flight schools for the hijackers to the first class plane tickets purchased for the flights on September 11th. The 19 hijackers engaged in financial transactions every day – paying rent, renting cars, buying food, and even sending small amounts of money back to the Persian Gulf just before the attacks – without ever being detected. It should be very apparent why. Our system was simply not created to catch those types of transactions. Our system was geared to a different purpose.

It should be obvious to all that the question that currently sits squarely with national policy makers in the United States is whether the systems we have built to ensure financial transparency – most of which were aimed at money laundering stemming from the illicit narcotics trade – are sufficient to provide the government with the information needed to vigorously track terrorist financing. As policy makers address these issues, allow me to state the obvious: it really is all about information.

Information is the lynchpin that holds together the ability to track terrorist financing. Some of this information is very sensitive information, developed through difficult and dangerous investigation or collection. So, if our systems are geared toward collecting information for a different set of problems, how can we collect the information needed to vigorously track terrorist financing? One tool provided by Title III of the U.S.A. PATRIOT Act found in Section 314 carries the mandate from the Congress to share information with the financial sector and to permit – through a safe harbor – financial sector members to share information with each other. So far, we have implemented this section by creating a “pointer” system for law enforcement. This pointer system gives law enforcement, in the right circumstances, the ability to work with FinCEN to transmit names of persons of interest to the financial sector to determine whether those institutions have any relevant transaction or account information. The industry reports back only when it has information, and then law enforcement follows-up with the institution with appropriate process. While this system is considered a success, and law enforcement has advised us it has been a valuable tool, I believe it is only an initial step in implementing our Congressional mandate to share information on a two-way basis with the financial industry. I believe the U.S. Congress was getting at something more profound.

Sharing relevant sensitive information with the financial sector in a deeper and richer way necessarily breaks several old and deeply entrenched paradigms. It brings the financial sector into a more collaborative relationship with the government. The genius of the mandate issued by the U.S. Congress is that it demonstrates that the old 20th Century paradigm of governments alone protecting their citizens from outside threats is no longer valid in a post-September 11th world. This paradigm, which has existed in one form or another since Pax Romana, simply no longer applies when enemies can melt into society and commandeer aircraft to use as missiles of devastation, or when a group of 28 thugs can take over a school and murder over 300 innocent souls with a brutality that has been rarely seen in modern times.

Deeper sharing of sensitive information with the financial sector also breaks the paradigm relating to the protection of information. We cannot enlist the help of the financial sector unless we can overcome the secrecy that envelops much of this information, whether it is information collected by the intelligence community or information developed by law enforcement. Much of relevant and useful information we would share typically comes from sources that have traditionally and automatically restricted access to small subsets of governmental personnel with a “need to know” rooted in Cold War perceptions of reality. These rules were created when “Spy vs. Spy” was the game nation states were playing.

Now, let me be clear. I understand that law enforcement is correctly reticent about sharing information critical to its investigations with anyone on the outside, just as intelligence services understandably guard their information to protect their sources and methods of obtaining the information. It is also true that some sharing of sensitive information is occurring with the financial sector, but it is usually occurring in a manner that is too *ad hoc* and generally occurring only when law enforcement or security services have leads that bring them to particular financial institutions. If the goal of our efforts is to vigorously track terrorist financing so we can identify, locate, and disrupt terrorists, their networks and their operations, then we must be willing to share sensitive information on a more systemic basis. This will not be easy. In addition to the real and legitimate governmental concerns about the protection of information, there are real and legitimate concerns about liberty and privacy. But I believe these concerns can be overcome – indeed, these concerns must be overcome if we are truly going to fight to win the “war” against terrorism. Our financial sector is more than eager to help. To be sure, I have witnessed that sector’s willingness to help time and again since September 11th.

It is also important to remember that the movement of money in the 21st Century knows no borders. Terrorism – particularly the type of terrorism we are dealing with since September 11th – has global reach as proven by the gruesome facts unfolding in Ossetia this past week. I would like to spend a minute or two to discuss the issue of information sharing, but in the context of the upcoming 10th anniversary in 2005 of what began as a small international meeting in Brussels that evolved into the Egmont Group of Financial Intelligence Units. In 1994, there were only a handful of operational units established pursuant to the Financial Action Task Force recommendation that nations set up a centralized entity to receive, review and make available to appropriate authorities financial transaction reports required by regulation and filed by financial institutions. The goals of that first meeting were to “start finding practical ways for information sharing and practicable solutions for eliminating barriers to such exchanges” among Financial Intelligence Units.

The Egmont Group has collectively accomplished much toward those goals, in a pretty spectacular fashion. Right now that original handful of “FIUs,” as they are known, has expanded to 94 nations that have made a commitment to put the resources in place to accomplish what FATF envisioned. The fact that 94 nations have done so is impressive in its own right, but consistent with my message to you today, what is even more important is that each FIU makes a commitment to sharing the information they collect

with other FIUs. I know it works. I have seen it in action. My organization, the Financial Crimes Enforcement Network, is the United States “Financial Intelligence Unit.” We have been a participant in the Egmont Group from the beginning and we host the Group’s secure website. My point is that when it comes to “breaking down barriers” to information sharing, the Egmont Group provides a model for how things can get done when there is an understanding that information becomes exponentially more valuable when it moves quickly to those who need it and can use it. I was heartened and enthused to hear the commitment to even greater information sharing that was made at the most recent plenary of the Egmont Group on the Isle of Guernsey this past summer. In my mind, that type of commitment is the type of commitment we need from policy makers to law enforcement to security services to regulators to break out of the old paradigms and address the threat we are all facing. We need to find ways of creating greater transparency in information flows among other governmental authorities and with the private sector to improve the odds that we will not be left in the dark when it comes to tracking terrorist financing.

Finally, if I may summarize, increasing financial transparency, both in the United States and the rest of the world is a key aspect to the global response to terrorism. It is absolutely imperative that we develop rules guaranteeing a certain level of financial transparency if we are to be effective at tracking terrorist financing. We all should applaud the good work of the FATF and the International Monetary Fund and World Bank on these efforts. Those institutions are making a very real difference in developing these rules. While multilateral consistency is essential in adapting international standards to the reality of tracking terrorist financing over the long term, we intend to use whatever tools we have available in situations where entities outside the U.S. are found to be knowingly supporting terrorism. One such tool is found in Section 311 of Title III of the USA PATRIOT Act. This provision provides the authority to protect the U.S. financial system from jurisdictions, institutions and types of financial transactions found to be of primary money laundering concern. In May of this year, the U.S. Treasury Department designated the Commercial Bank of Syria (CBS) as a financial institution of “primary money laundering concern” based on concerns that related to financial transparency, and problems we observed with that institution, including terrorist financing. While the use of Section 311 is meant to be a prophylactic measure – not a sanction – we believe that use of this tool will help convince jurisdictions and institutions to adopt real reforms that permit an acceptable degree of financial transparency. With appropriate restraint, we have applied this measure when we have reason to believe that our financial system is being threatened by terrorist financing or other criminal networks and we will continue to apply it. It is our hope that this measure will lead to greater financial transparency around the world.

I very much appreciate your kind attention this morning. I look forward to discussing with many of you these important issues and the other important issues that will be raised this week. Again, thanks to Professor Ryder, Mr. Froomkin and to Jesus College and Cambridge University for creating this terrific forum to discuss these critically important issues.